John A. Conkle (SB# 117849)
j.conkle@conklelaw.com
Amanda R. Washton (SB# 227541)
a.washton@conklelaw.com
CONKLE, KREMER & ENGEL
Professional Law Corporation
3130 Wilshire Boulevard, Suite 500
Santa Monica, California 90403-2351
Phone: (310) 998-9100 • Fax: (310) 998-9109

Michael M. Lafeber (*pro hac vice* pending)
mlafeber@taftlaw.com
O. Joseph Balthazor Jr. (*pro hac vice* pending)
jbalthazor@taftlaw.com
TAFT STETTINIUS & HOLLISTER LLP
2200 IDS Center
80 S. 8th St.
Minneapolis, MN 55402
Tel: 612.977.8400
Fax: 612.977.8650

Attorneys for Movant
Dexon Computer, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CISCO SYSTEMS, INC., and CISCO TECHNOLOGY, INC.,

Plaintiff,

v.

DEXON COMPUTER, INC.,

Defendant.

Case No. 3:20-cv-4926

DECLARATION OF STEPHEN O'NEIL IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

I, Stephen O'Neil, declare as follows:

1. I am the President and Chief Executive Officer of Dexon Computer, Inc. ("Dexon").

2. Dexon is a Minnesota corporation that was founded in 1992. I have worked there since its inception.

3. Dexon rents, sells, and services new, refurbished, and discontinued networking hardware. Dexon's offerings include routers, servers, switches, transceivers and phones.

4. Dexon has one office, which is in Bloomington, Minnesota. Its registered agent's address is in Minneapolis, Minnesota.

5. Dexon has 23 employees, all of whom physically work in Minnesota.

6. Dexon does not have any employees, offices, or service-of-process agents in California.

7. Dexon is not licensed to do business in California, owns no property in California, and pays no taxes there.

8. Dexon does not directly advertise in California. Specifically, Dexon does not run any print, television or radio advertisements with circulation in or near California.

9. Between July 1, 2017, and December 31, 2019, just 2.9% of Dexon's revenue from Cisco products involved customers with a California shipping address. Such products are often drop-shipped directly from Dexon's third-party suppliers and vendors.

10. I have reviewed the allegations made against Dexon in Cisco's complaint. Cisco has identified just two sales of allegedly counterfeit Cisco products by Dexon to end customers with a California address. Based on the allegations in the complaint, those transactions did not involve actual end consumers. Rather, they were "set ups" by Cisco investigators

11. Contrary to Cisco's efforts to falsely portray Dexon as a bad faith or willful counterfeiter, Dexon goes to great lengths to attempt to avoid counterfeit products. To the extent any Cisco products sold by Dexon are ultimately proven to be counterfeit, Dexon is merely an innocent victim of the unfortunate fact such counterfeit products have found their way into the market. Cisco's own authorized partners and sellers are likewise often the victim of counterfeit products. Attached as **Exhibit A** is a true and correct copy of an article about the sale of counterfeit Cisco products to the U.S. Government by an authorized Cisco partner.

12. Attached as **Exhibit B** is a true and correct copy of the April 15, 2020 order from the United States District Court, District of Minnesota granting in-part and denying in-part Cisco's motion to compel, Cisco's memorandum of law in support, and Dexon's memorandum of law in opposition.

I declare under penalty of perjury that to the best of my knowledge the foregoing statements are true and correct.

Dated: September 25, 2020

/s/Stephen O'Neil
Stephen O'Neil

Exhibit A

Cisco partners sell fake routers to US military

Cisco admits its partners sold counterfeit Cisco products to the US military, posing a serious threat to military and critical national infrastructure, according to the FBI

By Tom Espiner | May 14, 2008 -- 23:59 GMT (16:59 PDT) | Topic: Cisco

Cisco admits its partners sold counterfeit Cisco products to the US military, posing a serious threat to military and critical national infrastructure, according to the FBI.

The counterfeit products could open a hardware backdoor into those systems, warned the Federal Bureau of Investigation (FBI), enabling an attacker, potentially undetected by security software, to gain control of the systems. Counterfeit parts also have a much higher failure rate: one is known to have caught fire in a government network, due to a faulty power supply, warned the FBI.

The FBI does not know whether the fake goods are made for private profit or are state-sponsored, nor the scope of counterfeit-equipment use in the US government. The FBI did warn, however, that there is a threat of IT subversion and supply-chain attack which could cause vital systems to fail, allow access to otherwise secure systems and weaken cryptographic safeguards on government data.

An FBI PowerPoint presentation leaked in April to abovetopsecret.com gave details of an FBI investigation into Cisco routers: "Operation Cisco Router". In the presentation, the FBI detailed how counterfeit Cisco goods from China had made their way into the US military supply chain.

Manufactured in the Shenzhen province of China, the fake Cisco equipment was then supplied directly to the US government through several routes: either directly through US distributors or through those who had bought the counterfeit kit off eBay; through distributors in other countries, including the UK; and through US government employees buying through

non-General Services Administration (GSA) approved sources. The GSA is the US federal acquisition agency.

One company was indicted in December 2007 for allegedly shipping counterfeit products from China and selling them to the Marine Corps, the Air Force, the Federal Aviation Administration, the FBI itself, defence contractors, universities and financial institutions.

The US Navy and Bonneville Power Administration, which serves the US Pacific Northwest with power, were allegedly sold counterfeit products by another company buying directly from China.

According to a whitepaper by the Alliance for Gray Market and Counterfeit Abatement (AGMA) and KPMG, approximately 10 percent of IT products sold are counterfeit. However, the FBI presentation said that law-enforcement agencies estimate the percentage to be higher.

The FBI presentation said part of the problem lies with government procurement practices, revealing that the government normally searches for the lowest prices for products. A counterfeit Cisco 1721 router costs $234 (Â£120), while the genuine version costs approximately $1,375. Another part of the problem is that government contracts allow for several levels of sub-contractors and non-OEM purchases, according to the presentation.

The FBI said there was little or no vetting of vendors or partners by the organisations. It was "gold" and "silver" Cisco partners who had been selling the counterfeit products to the government, said the FBI.

Cisco on Tuesday admitted that some of its partners had sold counterfeit goods but said the majority of its certified channel partners had not sold counterfeit Cisco products. The company instead blamed the "grey market" of semi-legal deals for most of the problems.

"It is important to note that the grey market and unauthorised channel partners account for the vast majority of the purchase and sale of counterfeit Cisco products," John Donovan, managing director of channels for Cisco UK, told *ZDNet.com.au*'s UK sister site ZDNet.co.uk in an email statement. "We actively and closely monitor our certified channel partners regarding this issue and will take strong measures against violators, [up] to and including decertification of a channel partner."

While admitting the problem in the US, Cisco, at the time of writing, had not said how widespread the problem of counterfeit goods being supplied to government was in the UK and in Europe. However, the FBI has been co-ordinating investigations into counterfeit Cisco products in the UK and Germany, according to the presentation.

Cisco did, however, comment on "Operation Cisco Router" in the US.

"Cisco has been extremely active throughout this collaborative effort with the FBI and other federal law-enforcement agencies from day one," wrote Donovan. "We appreciate the hard work by the FBI in this case, as well as the efforts by all law-enforcement agencies, in cracking down on the counterfeit market. In this instance, we have participated throughout the investigation in all aspects, including executing search warrants, [and] we have proactively briefed high-level individuals across multiple agencies so that they are aware of this ongoing challenge in the IT industry, as well as Cisco's co-operation in this particular investigation."

One of the criticisms levelled by the FBI was that Cisco's brand-protection team, which monitors counterfeiting, did not co-ordinate with Cisco's government-sales team. Cisco had not commented on this criticism at the time of writing, instead saying: "As part of our commitment to the integrity and quality of Cisco technology and services, our brand-protection team maintains an on-going, pro-active and company-wide effort to minimise potential damage to our brand and to our customers as a result of counterfeiting."

Cisco said that buyers of equipment purporting to come from Cisco who are concerned about counterfeit products should look for signs, such as prices that seem too good to be true; equipment without a valid software licence, where applicable, or which does not enclose a Cisco warranty; increased failure rates; and packaging that is not original or appears to have been used before or tampered with.

"If you think something suspicious is going on, we encourage you to contact your nearest Cisco office," said Donovan.

RELATED TOPICS: NETWORKING TECH INDUSTRY INTERNET OF THINGS CXO CLOUD

Exhibit B

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

CISCO SYSTEMS, INC. and CISCO TECHNOLOGY, INC.,

Movants,

v.

DEXON COMPUTER, INC.,

Respondent.

No. 0:20-mc-00030-NEB-KMM

ORDER

This matter is before the Court on Cisco Systems, Inc., and Cisco Technology, Inc.'s (collectively "Cisco") Rule 45 Motion to Compel. [Mot., ECF No. 1.] Cisco seeks to compel Dexon Computer, Inc. ("Dexon"), to produce documents pursuant to a subpoena Cisco served in connection with underlying litigation in the Norther District of California.[1] [Nelson Decl., Ex. B.] Dexon opposed the motion on several grounds. [Dexon Mem., ECF No. 18.] The Court held a telephonic hearing on April 14, 2020, at which both Cisco and Dexon appeared through counsel. [Mins. of Hr'g, ECF No. 26.] The Court made several rulings on the record and carefully explained its reasoning. The rulings themselves are memorialized in this Order.

1. Cisco's Rule 45 Motion to Compel **[ECF No. 1]** is **GRANTED IN PART** and **DENIED IN PART** as stated on the record at the hearing.

2. The time period for the documents Dexon is ordered to produce by this Order is December 18, 2015, through the present.

---

[1] In the underlying litigation, Cisco accuses several defendants, referred to in this proceeding as "the Sheikh entities," of importing and selling counterfeit Cisco products in violation of the Lanham Act and other statutes. *See Cisco Systems, et al. v. Zahid "Donny" Hassan Sheikh, et al.*, Case No. 4:18-cv-07062-YGR (N.D. Cal. filed Dec. 4, 2019); [Nelson Decl., Ex. A, ECF No. 4-1.]

3. Dexon shall produce documents showing its purchases of Cisco-branded switches from PureFuture Tech, LLC ("PFT"), that were acquired from or originated from HongKong Sellsi ("HKS"). Dexon shall also produce documents showing its subsequent sales of such products. Dexon shall make every effort to produce the documents discussed in Paragraph 3 of this Order (the HKS switches) by April 21, 2020, but must make the production no later than April 28, 2020.[2]

4. Dexon shall produce documents showing its purchases of Cisco-branded transceivers from PFT that were acquired from or originated from Pretty Technology or Wuhan Etop Com. Dexon shall also produce documents showing its subsequent sales of such products. Dexon shall produce these documents no later than April 28, 2020.

5. For the Cisco-branded switches discussed in Paragraph 3 of this Order, Cisco is permitted to contact the end-users or customers to which Dexon distributed such products. Cisco and Dexon are required to meet and confer immediately to discuss the means of this communication and to make all reasonable efforts to ensure that such communications protect Dexon's legitimate business interests. Any disagreements regarding this process must be promptly brought to this Court's attention through an informal discovery dispute resolution procedure. The party seeking a ruling from the Court must file a letter of no more than three pages, and the opposing party may respond within 48 hours. The Court will either issue its ruling based upon the written submissions or promptly set a telephone conference to discuss the matter.

[2] In light of the current fact-discovery deadline of May 1, 2020 in the underlying litigation, counsel for Cisco and Dexon are encouraged to continue their efforts at compromise and cooperation.

6. For the Cisco-branded transceivers discussed in Paragraph 4 of this Order, at this time, Cisco is not permitted to contact the end-users or customers to which Dexon distributed such products.

7. Dexon shall produce documents concerning any customer complaints for the switches and transceivers discussed in Paragraphs 3 and 4 of this Order.

8. Dexon shall produce documents showing any communications it had with PFT regarding the switches and transceivers discussed in Paragraphs 3 and 4 of this Order.

IT IS SO ORDERED.

Date: April 15, 2020

s/Katherine Menendez
Katherine Menendez
United States Magistrate Judge

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MINNESOTA

CISCO SYSTEMS, INC. and CISCO TECHNOLOGY, INC., Plaintiffs, v. DEXON COMPUTER, INC. Defendant.	Civil Action No.

MEMORANDUM OF LAW IN SUPPORT OF CISCO SYSTEMS, INC. AND CISCO TECHNOLOGY, INC.'S RULE 45 MOTION TO COMPEL NONPARTY DEXON COMPUTER, INC. TO COMPLY WITH SUBPOENA TO PRODUCE DOCUMENTS

This is a motion to compel filed as part of an ongoing case in the United District Court for the Northern District of California, *Cisco Systems, et al. v. Zahid "Donny" Hassan Sheikh, et al.*, Case No. 4:18-cv-07602-YGR, pending before Judge Yvonne Gonzalez Rogers (the "Underlying Case"). A true and correct copy of the operative Complaint in the Underlying Case is attached as Exhibit A to the Declaration of Richard J. Nelson in Support of Cisco's Motion to Compel ("Nelson Decl."), filed concurrently herewith.

Plaintiffs Cisco Systems, Inc. and Cisco Technology, Inc. (together, "Cisco") hereby move for an order under Federal Rule of Civil Procedure 45, compelling non-party Dexon Computer, Inc. ("Dexon") to comply with Cisco's subpoena to produce documents. A copy of the subpoena is attached as Exhibit B to the Nelson Declaration.

If the subpoenaed party objects to producing documents, "the serving party may move the court for the district where compliance is required for an order compelling production or inspection." Fed. R. Civ. P. 45(d)(2)(B)(ii). Because Dexon is located in Minneapolis, Minnesota, this Court has jurisdiction to hear this motion. Cisco has met

and conferred with counsel for Dexon, but Dexon has still unreasonably refused to comply with the subpoena, necessitating this motion.

I. INTRODUCTION

Cisco issued a subpoena to non-party Dexon for purchase and sales documentation and communications related to potentially counterfeit products Dexon purchased from the defendants in the Underlying Action and resold to end-users. Dexon responded to Cisco's subpoena by raising blanket confidentiality, relevance, and burden objections. Cisco offered in a good-faith attempt to cooperate with Dexon to narrow its requests and address Dexon's concerns. Dexon nevertheless continued to refuse to produce any documents to Cisco unless Cisco agreed that Dexon's production of approximately 100 purchase orders (without sales information or communications) would completely satisfy its obligations under the subpoena. Notably, Dexon refused to provide documents showing where the products sold by the defendants are currently located—effectively depriving Cisco of the ability to prove its case in the Underlying Action by inspecting the products to determine if they are counterfeit. To date, Dexon has not produced a single document to Cisco. The Court in the underlying case in Northern District of California has set a fact discovery cutoff for March 20, 2020.[1]

II. FACTUAL BACKGROUND

Cisco is a worldwide leader in developing, implementing, and providing networking, communications, and information technology products and services. Cisco products handle electronic communications by and in large and small business and critical infrastructure (such as the US military, State Department, air traffic control,

[1] When the Court set this cutoff, counsel for Cisco advised the Court that there was third-party discovery that was still pending, including its subpoena to Dexon. The Court invited counsel to bring any issue about receiving the discovery to her by March 20, should extensions be necessary. Nelson Decl., ¶ 4. Thus, the fast approaching discovery cutoff date should not pose an issue if Dexon were to be ordered by this Court to produce the documents even after March 20.

banks, and hospitals). *See* Nelson Decl., Exh. A, ¶¶ 22, 28, 32-33. On December 18, 2018, Cisco brought counterfeiting and trademark infringement claims against a number of related entities and individuals in the Northern District of California. Cisco alleges, *inter alia*, that Defendants Advanced Digital Solutions International, Inc. ("ADSI"), K & F Associates, LLC ("K & F"), and PureFutureTech LLC("PFT") (together, the "Sheikh Entities") knowingly and intentionally engaged in a massive scheme to import and sell counterfeit Cisco products in the United States.[2] *See generally* Nelson Decl., Ex. A at pp. 7–14, 17.

Cisco propounded discovery on the Sheikh Entities. Nelson Decl., *at* ¶ 5. In response to Cisco's request for production of documents, PFT produced invoices for Cisco products that PFT sold to Dexon, a networking hardware supplier/reseller located in Bloomington, Minnesota. *Id.*; *see also* Nelson Decl., Ex. C. Many of the transactions involved products purchased by the Sheikh Entities from HongKong Sellsi ("HKS"), an entity in China that has sold numerous counterfeit Cisco products into the United States. Nelson Decl., Ex D at ¶¶46-58, *Id.*[3] Of particular note and concern are unknown components soldered onto the Cisco motherboard by HKS, as depicted in *Id.*, ¶ *55:*

[2] ADSI, K & F, and PFT are owned by members of the Sheikh family, including Shahid Sheikh, and run by the family, including Shahid Sheikh, Kamran Sheikh, and Farhaad Sheikh, who are named individually as defendants in the underlying litigation. The Sheikh family often used the Sheikh Entities interchangeably in the purchase and sale of Cisco products.

[3] Cisco sued HKS with regard to its sales of counterfeit Cisco products in a separate litigation in the Northern District of California. *Id.* at ¶ 7, Ex. D. The allegations against HKS were serious—including that HKS soldered mysterious components onto motherboards for switches that were communicating electronic information in the end user's networks. *See generally id.* at Ex. D, pp. 14–22. In fact, some of HKS's Cisco switches, with the mysterious components, were located at a federal credit union in Nevada. *See* Nelson Decl., Ex. at pp.

The documents that Cisco subpoenaed from Dexon would permit Cisco to locate the HKS switches and other potentially counterfeit products sold by the Sheikh Entities to Dexon, and identify where the products are so that they can be analyzed to determine whether they are genuine or counterfeit.[4] This evidence is clearly relevant in the litigation against the Sheikh Entities (as they sold the counterfeit switches to Dexon). Below is a chart showing the known transactions between the Sheikh Entities and Dexon:

Date of Sale to Dexon	**Seller to Sheikh Entities**	**Products**
3/14/18	HKS	5 WS-C2960X-48FPD-L switches
4/10/18	HKS	2 WS-C3650-48PS-E switches
5/22/18	HKS	3 WS-C3850-48T-E switches
6/1/18	HKS	12 PWR-C1-1100W power supplies
6/20/18	K&F	4 WS-C2960XR-48FPD-L switches
7/10/18	HKS	5 WS-C2960X-48FPD-L switches
2/26/2018	Pretty Technology (China)	8 40G QSFP+ Active Optical Cable; 3 40GBASE-CR4 Active Copper Cable
8/8/18	"T2 Systems Co." (Hong Kong)	2 WS-C3850-12X48U-L switches
12/7/18	Unstated (Hong Kong)	2 AIR-AP28021 wireless access points
12/18/18	RonTech Ltd. (Surrey, UK) Unstated (China)	17 WS-C2960X-48FPD-L switches

See Nelson Decl., Ex. C.

[4] Based on the known information about HKS and other Chinese sellers of "Cisco" products, it is very likely that the products are counterfeit, but Cisco nevertheless seeks to examine them to obtain more concrete proof for use in the Underlying Case.

There is a strong likelihood that the products sold by the Sheikh Entities to Dexon are counterfeit. A former employee testified in a recent deposition that the Sheikh Entities arranged for a shipment location hundreds of miles away from their office, to which they imported Cisco products from China. Notably, they received other brands, such as HP, directly to their office, but the Cisco products from China were received at the Reno location, far from ADSI's office. Nelson Decl., ¶ 19. In addition, the former employee testified that once the products were received by the Sheikh entities, other employees would affix counterfeit labels on them, and then sell the products to the US government and other customers (which would include Dexon). *Id.*

Because PFT's records did not identify the end customer for the products Dexon purchased, and because Cisco therefore could not examine the products to determine their genuineness, Cisco issued a subpoena to Dexon on July 17, 2019 for: (1) purchase and sales data (dates of purchase/sale, product IDs, serial numbers, and purchase and sale prices) related to Cisco products it purchased from the Sheikh Entities (Request Nos. 1–6), (2) communications Dexon had with the Sheikh Entities (Requests Nos. 7–9), and (3) all customer complaints related to Cisco products Dexon purchased from the Sheikh Entities (Request Nos. 10–12). *See* Nelson Decl., Ex. B. The subpoena was served on Dexon on July 29, 2019. *Id.*

On August 12, 2019, counsel for Dexon responded to Cisco, raising a number of objections to Cisco's subpoena. *See* Nelson Decl., Ex. E. Specifically, Dexon objected that (1) the documents sought are available from the Sheikh Entities themselves and that requiring Dexon to produce the documents is therefore unduly burdensome (as to Request Nos. 1–9); (2) the document sought contain confidential, proprietary, and trade secret information (as to all requests); and (3) the discovery sought is neither relevant nor proportional to Cisco's claims (as to all requests). *Id.*

However, over the course of many months of telephone calls and emails, it became clear that Dexon's true reason for resisting the subpoena was to prevent any contact with its customers about the potentially counterfeit products that Dexon

purchased from the Sheikh Entities. During Cisco and Dexon's initial meet-and-confer telephone call in August 20, 2019, Cisco explained that it believed the products Dexon purchased from the Sheikh Entities were likely counterfeit (due to fact that HKS and other foreign companies were the sources) and that the subpoena request would allow Cisco to locate and analyze the authenticity of products that the Sheikh Entities sold to Dexon. Nelson Decl. at ¶ 9. However, Dexon requested that Cisco provide additional documentation related to specific products Cisco believed to have come from HKS or other foreign companies before it would agree to turn over any documents. *Id.*

On the same day, Cisco provided invoices showing the PFT products sold to Dexon originated from HKS and other Chinese sources. *Id.* at ¶ 10, Ex. F. Dexon did not respond. Cisco continued to follow up with Dexon over the next few months. *Id.* at Ex. G.

The parties scheduled another phone call in November 2019 in which Dexon confirmed that it had approximately 100 purchase orders with PFT. *Id.* at ¶ 12. Dexon expressed concern that any attempts to contact its customers about the genuineness of Cisco products would harm its customer relationships. *Id.* Based on the parties' conversation, Cisco agreed to accept the 100 purchase orders from PFT and not to seek Dexon's sales records or customer information at that time, reserving the right to reopen discussion of the issue after reviewing the purchase orders. *Id.*. Cisco attempted to confirm this agreement with Dexon in writing through email, but Dexon did not respond. *Id.* at Ex. G. Cisco continued to follow up. *Id.*

On February 12, 2020, Dexon represented that it was "willing to produce the relevant purchase orders subject to appropriate terms/restrictions". *Id.* at ¶ 13. The parties arranged another phone call. *Id.* Rather than being concerned that it may have sold counterfeit products to its customers, Dexon was adamant that it would not produce any documents that would identify where the products are currently located, again claiming that any customer contact would damage Dexon's customer relationships. *Id.* To assuage Dexon's concerns, Cisco agreed that it would not contact Dexon's customers

without first consulting with Dexon, but reserved the right to revisit, should the need arise. *Id.* Cisco also offered Dexon a cooperation agreement, whereby Cisco would release claims against Dexon for the sale of counterfeit products in return for Dexon's assistance in identifying and replacing any counterfeit products Dexon may have sold. Nelson Decl., Ex. H. Under the agreement, Cisco proposed to allow Dexon to handle the communications with Dexon's customers, and the parties would agree on any messaging to customers about the counterfeiting issue beforehand. *Id.*

Rather than accept Cisco's reasonable solution, Dexon refused to provide any documents, save for the purchase orders with PFT, and only if Cisco would agree that production of the purchase orders would fully satisfy Dexon's obligations under the subpoena. *Id.* at Ex. G. Cisco attempted one last time to schedule a meet-and-confer telephone call with Dexon on March 10, 2020. Nelson Decl., Ex. I. Cisco counsel explained that information about where the products are now was critical to Cisco's case against the Sheikh Entities, because it allows Cisco to locate the sold products and test them to determine if they are counterfeit, which is central to Cisco's claims and damages. Dexon's counsel stated that he did not have authority to alter Dexon's prior position, and said that he would alert Cisco if Dexon changed its mind by the end of the day on March 11. *Id.* at ¶ 14. When Dexon did not change its position, Cisco was left with no choice but to bring this motion to compel.

III. LEGAL ANALYSIS

"Pursuant to a subpoena, a non-party can be compelled to produce evidence regarding any matter relevant to the claim or defense of any party, unless a privilege applies." *United States v. R.J. Zavoral & Sons, Inc.*, No. 12-CV-668 (MJD/LIB), 2014 WL 12756820, at *3 (D. Minn. Jan. 17, 2014). Relevance is construed broadly, but document requests must also be "proportional to the needs of the case". *See* Fed. R. Civ. P. 26 (b)(1) (listing factors for determining proportionality). As detailed below, Dexon has objected to Cisco's subpoena without providing any legitimate justification for doing so.

A. Cisco's Requests Are Directly Relevant and Proportional to Cisco's Claims (All Requests)

It cannot be reasonably disputed that Cisco's subpoena seeks information relevant to Cisco's counterfeiting claims against the Sheikh Entities: Cisco alleges that the Sheikh Entities imported counterfeit Cisco products and sold them in the United States. *See* Nelson Decl., Ex. A at ¶¶ 34-72. Cisco's requests are narrowly tailored to seek purchase and sales information related to products Dexon purchased from the Sheikh Entities, communications with the Sheikh Entities about Cisco products, and customer complaints about products Dexon purchased from the Sheikh Entities. These requests are directly relevant to how many products the Sheikh Entities sold, what representations the Sheikh Entities made to their customers about the products they were selling, and whether Dexon ultimately received any complaints from end customers that would indicate that the products the Sheikh Entities sold were in fact counterfeit. Importantly, the requests would also allow Cisco to locate the actual products the Sheikh Entities sold and analyze them to determine whether they are indeed counterfeit, which goes to the heart of Cisco's case, which alleges Lanham Act counterfeiting causes of action.

Cisco's requests are also proportional to the case, especially when considering that the information Cisco seeks, which relate to the ultimate issue of whether the products the Sheikh Entities sold were counterfeit, is solely in Dexon's possession (i.e., not available from the Sheikh Entities or other defendants in the case). Cisco's requests are also narrowly tailored in time for purchases and sales from December 18, 2015 onward; are limited only to Cisco products; and seek data that should be easily retrievable and accessible to Dexon through their sales platform or other electronic platforms (e.g., searching an email inbox for the terms "Cisco" and the three Sheikh Entities).

Dexon has not provided any specific facts as to how responding to Cisco's requests would be unduly burdensome. *See Deluxe Fin. Servs., LLC v. Shaw*, No. 16-CV-3065 (JRT/HB), 2017 WL 7369890, at *4 (D. Minn. Feb. 13, 2017) ("[The]

objecting party will ordinarily have better information about burden or expense."). Indeed, Dexon appeared to have been able to easily determine that it had only approximately 100 purchase orders involving PFT and had not purchased any products from the remaining Sheikh Entities. The relatively small number of applicable purchase orders (and presumably therefore a relatively small number of related sales) indicate that producing information about those purchases and sales, and any information related thereto, would not be overly burdensome.

B. Responsive Documents Are Not Available From the Sheikh Entities (Request Nos. 1–9)

While courts must afford particular consideration to burdens placed upon nonparties, there is no rule that parties must only seek documents available to defendants. *See Deluxe Fin. Servs., LLC v. Shaw*, No. 16-CV-3065 (JRT/HB), 2017 WL 7369890, at *5 (D. Minn. Feb. 13, 2017) (enforcing subpoena that sought from third party all communications between third party and defendant). Here, the bulk of records exist only with Dexon—their sales orders to the customers that identify where the presumptively counterfeit products currently are located and customer complaints about potentially counterfeit Cisco products.

As to Dexon's purchase records, Cisco has conducted discovery with PFT, and so this is not a situation where a party has not first sought the documents from the other parties in the litigation. Moreover, Dexon may have also captured additional information about its purchased products that PFT did not. For example, PFT's sales documents did not capture the serial numbers for their products. Third-party resellers often log serial numbers to identify the products they purchase and sell in case an end customer wants to return the product or submits a complaint. This information is not available from PFT, and can be very useful in determining whether a product is counterfeit. Nelson Decl., ¶ 17.

As to Dexon's communications with the Sheikh Entities, "[n]o rule requires the requesting party to seek discovery from only one party to any given conversation. *Deluxe Fin. Servs., LLC v. Shaw*, 2017 WL 7369890, at *5. None of the Sheikh Entities produced any communications with Dexon. *See id.* ("[Defendant] Shaw, for example, may not have kept copies of the same communications that [subpoenaed non-party] Johnson did."). Dexon provided no information as to whether Dexon has any communications with the Sheikh Entities or how searching for the requested communications would be unduly burdensome. Cisco is willing to work with Dexon on determining suitable search and custodian parameters as well as timeframes for Request Nos. 7–9, as necessary.

As to Dexon's sales records and customer complaints, there is no reason to expect the Sheikh Entities or any other entity to have access to those types of documents. Presumably, Dexon keeps its sales and RMA records in an easily searchable electronic database, and Dexon has provided no information to the contrary.

C. Dexon's Records May Be Produced Under the Protective Order (All Requests)

Cisco recognizes that some of the information it seeks from Dexon, while not rising to the level of being proprietary or trade secret information, may indeed be viewed as commercially sensitive by Dexon. However, the Court in the underlying litigation has issued a protective order that extends to non-party documents which should more than adequately address Dexon's confidentiality concerns. *See* Nelson Decl., Ex. J; *Datcard Sys., Inc. v. PacsGear, Inc.*, No. 11MC25 DSD/SER, 2011 WL 2491366, at *2 (D. Minn. June 23, 2011) (finding protective order "affords substantial protection" to confidential and proprietary information provided by third party and denying order to quash subpoena).

Here, the evidentiary value of the sales and customer complaint information that Cisco seeks more than outweighs the purely theoretical potential harm to Dexon and its customer relationships. Information related to the genuineness or counterfeit nature of

the products PFT sold to Dexon, and which Dexon subsequently sold to consumers, goes to the heart of Cisco's counterfeiting claims. Second, any harm caused by contacting Dexon's customers (who presumably did not want to purchase counterfeit products and would want to have any counterfeit products replaced) would be mitigated by Cisco's prior agreement to work with Dexon to carefully craft any messaging to Dexon customers to avoid harm, and to permit Dexon to be the entity that makes the contact.[5]

IV. CONCLUSION

The information Cisco requests from Dexon is highly relevant to Cisco's counterfeit claims against the Sheikh Entities and other defendants, providing an essential avenue by which Cisco can analyze the counterfeit nature of products the Sheikh Entities sold. Dexon provides no justifiable reason for withholding responsive documents. Cisco therefore respectfully requests that the Court order Dexon to search for and produce all documents responsive to Cisco's requests.

[5] Cisco offered such an arrangement as a courtesy to Dexon and in a good-faith effort to assuage Dexon's concerns. However, Cisco would be well within its rights to subpoena Dexon's customers without needing to obtain Dexon's consent.

DATED: March 13, 2020

/s/ David P. Swenson
David P. Swenson
Larkin Hoffman Daly & Lindgren, Ltd
8300 Norman Center Drive
Suite 1000
Minneapolis, Minnesota 55437
Phone: (952) 835-3800
Fax: (952) 842-1746
dswenson@larkinhoffman.com

Pending Admission Pro Hac Vice:
Richard J. Nelson
rnelson@sideman.com
Anna P. Chang
achang@sideman.com
Sideman & Bancroft LLP
One Embarcadero Center, 22nd Floor
San Francisco, CA 94111
(415) 392-1960

Attorneys for CISCO SYSTEMS, INC. and
CISCO TECHNOLOGY, INC.

4837-4475-7943, v. 2

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Cisco Systems, Inc., and Cisco Technology, Inc. Plaintiffs, v. Dexon Computer, Inc. Defendant.	)))))))))	Civil No. 0:20-mc-00030-NEB-KMM **MEMORANDUM IN OPPOSITION TO CISCO SYSTEMS, INC. AND CISCO TECHNOLOGY, INC.'S RULE 45 MOTION TO COMPEL NONPARTY DEXON COMPUTER, INC. TO COMPLY WITH SUBPOENA TO PRODUCE DOCUMENTS**

I.
INTRODUCTION

Dexon Computer, Inc. ("Dexon") submits this memorandum in opposition to Cisco Systems, Inc.'s and Cisco Technology, Inc.'s ("Cisco") motion to enforce a subpoena to produce documents. Cisco's motion is both untimely and substantively lacking.

Cisco served the subject subpoena on July 29, 2019. Belying its current argument that the requested documents are important to its underlying case, Cisco inexplicably waited approximately eight (8) months, and days prior to the expiration of the extended fact discovery deadline, to bring the present motion. Fact discovery is currently *closed* in the underlying Northern District of California litigation and Cisco's motion therein for leave to conduct the very discovery at issue in the present motion has been opposed and remains pending.

In addition to its untimeliness, Cisco's motion is substantively flawed. Namely, Cisco has failed to demonstrate any need for the requested documents which overcomes the severe burden and harm caused to Dexon by revealing its confidential and trade secret

information. Rather, Cisco has put forth disjointed allegations that some de minimis portion of Dexon product allegedly sourced from HongKong Sellsie ("HKS") was counterfeit. At best, Cisco's motion demonstrates that the requested Dexon documents have little or no relevance or value to the underlying litigation, but rather are merely duplicative to information already in Cisco's possession or readily available from other sources, including the actual parties to the litigation.

II.
BACKGROUND

A. Cisco's Motion is Untimely

Cisco failed to diligently and timely pursue the documents it now seeks from Dexon. The underlying counterfeiting litigation was commenced in the Northern District of California more than fifteen (15) months ago on December 18, 2018. Dkt. 4, p.3. Cisco served Dexon with the subject subpoena approximately eight (8) months ago on July 29, 2019. Dkt. 4-1, pp. 29-39.

The fact discovery deadline in the underlying litigation was originally set for January 20, 2020, and has already been extended once to March 20, 2020. Cisco argues the now-expired March 20, 2020 discovery cut-off date "does not pose a problem." *See* Dkt. 3, p. 2, n.1 ("When the Court set this cutoff, counsel for Cisco advised the Court that there was third-party discovery that was still pending, including its subpoena to Dexon. The Court invited counsel to bring any issue about receiving the discovery to her by March 20, should extensions be necessary. . .Thus, the [March 20, 2020] discovery cutoff date should not pose an issue. . .").

Contrary to Cisco's claim, it failed to mention the Dexon subpoena in the parties' February 14, 2020 Joint Case Management Conference Statement seeking to extend the fact discovery deadline to March 20, 2020. Rather, Cisco's sole expressed concerns related exclusively to "various government end customers." ("Cisco is agreeable to [the March 20, 2020] cutoff date, but. . .there is third party discovery that might not be completed by this date. Specifically, Cisco is subpoenaing various *government end customers* that purchased Cisco products from the ADSI Defendants, to examine the products and get documents. Cisco is acting diligently to complete this discovery, but it would like to alert the Court that it may seek to complete certain third party discovery after the discovery cutoff, if that becomes necessary.") (italics added). Declaration of Michael M. Lafeber, Exhibit A., p. 2, n.1.

On March 20, 2020, the last day of the extended discovery period, Cisco filed a motion seeking leave to conduct certain third party discovery subsequent to the discovery cut-off date.[1] Cisco's motion for leave has been opposed by Defendants, in part due to Cisco's failure to diligently pursue such discovery; and in part due to the fact that the requested discovery will inevitably lead to even *further* discovery in light of Cisco's expressed intent to contact identified end consumers and conduct product testing. Lafeber Dec., Ex. D.

[1] Such motion for leave identifies the Dexon subpoena. Lafeber Dec., Ex. B. The Declaration of Attorney Richard Nelson supporting such motion for leave indicates Cisco first mentioned the Dexon subpoena to the California court as part of a Case Management Conference on February 19, 2020. Lafeber Dec., Ex. C.

Cisco misleadingly suggests, both herein and its motion for leave pending in the Northern District of California, that it has been actively involved in negotiations with Dexon for the past eight (8) months, and/or that Dexon is somehow responsible for the tardy nature of the present motion. In fact, as a result of good faith "meet and confer" efforts, Cisco originally indicated one of the reasons for the subject subpoena was to attempt to confirm whether the Dexon related sales records produced by underlying Defendant PureFutureTech, LLC ("PFT") were complete and accurate. To that end, Dexon indicated it was amenable to producing its PFT purchase orders. (PFT is the sole entity identified in Cisco's subpoena which Dexon dealt with or purchased product from.) At all times, Dexon made it clear it was not willing or amenable to disclosing the identity of its end customers in light of Cisco's expressed intent to contact such customers, disparage Dexon, require such customers to subject their products to testing, and drag such customers into the underlying Northern District of California litigation. (Lafeber Dec. ¶¶1-2)

Despite initially accepting Dexon's limiting proposal, Cisco's confirming communication made it clear Cisco wanted a "one way" or unilateral agreement. Namely, Cisco wanted Dexon to voluntarily produce its PFT purchase orders, while Cisco reserved all of its rights to seek further documentation and information, including information identifying Dexon's customers. Knowing full well Dexon was not amenable or agreeable to such a proposal, Cisco inexplicably delayed *months* to attempt to enforce the subpoena, filing the present motion just days prior to the expiration of the extended March 20, 2020 discovery cut-off date. (Lafeber Dec. ¶¶3-4)

B. Requested Documents Overbroad, Unnecessary and/or Duplicative

1. Alleged HongKong Sellsi ("HKS") Counterfeit Products

Cisco's moving papers argue the purpose of the Dexon subpoena is to confirm products sourced from HKS were counterfeit. Dkt. 3, p. 3 ("Many of the [Dexon] transactions involved products purchased by the Sheikh Entities from [HKS], an entity in China that has sold numerous counterfeit Cisco products into the United States."); *id.* ("Of particular note and concern are unknown components soldered onto the Cisco motherboard by HKS. . ."); *id.* at p. 4 ("The documents that Cisco subpoenaed from Dexon would permit Cisco to locate the HKS switches. . .").

Cisco's pending Northern District of California motion for leave further confirms the Dexon subpoena is limited to identifying HKS sourced products. Cisco's memorandum in support of such motion states:

> Based on the discovery conducted with the Defendants, it became clear that the Defendants imported Cisco products from a Chinese company, [HKS], and then sold those products to Dexon. The 'Cisco' products sold by HKS are particularly worrisome, because they include unknown components soldered onto the motherboards of Cisco switches, which are used to manage electronic communications for sensitive government and other infrastructure. . .If the court in Minnesota orders Dexon to comply with the subpoena, Dexon will produce documents that show where the HKS products currently are. In other words, it will allow Cisco to trace the products from HKS, to the ADSI Defendants, to Dexon, to the customer that has the potentially counterfeit product."

Lafeber Dec., Ex. B, p. 2.

Dexon understandably initially inquired about Cisco's basis for believing any Dexon products acquired from PFT originated with HKS. In response, Cisco acknowledged that only limited Dexon related documents produced by PFT could be traced

to HKS. By way of email dated August 20, 2019, Cisco's counsel provided the Dexon related documents produced by PFT. The documents were provided via two separate pdf's labeled "Dexon Invoice – HKS" and "Dexon Invoices – non HKS." The email explained that the first set was for products sourced from HKS, while the second set was for products admittedly not sourced by HKS. Lafeber Dec., Ex. E. ("Per our phone call today, attached please find two sets of invoices referencing Dexon (one set of invoices for products sourced from HongKong Sellsi and one set of invoices for products from other sources in China.")

Consistent with the previously produced invoices, Cisco's motion is able to identify just four (4) alleged Dexon transactions with PFT involving the allegedly counterfeit HKS switches. (Cisco identifies a fifth purported transaction purportedly sourced from HKS involving a "power supply" Dkt. 3, p. 2.)

Despite this fact, Cisco's subpoena is in no way limited to the four (4) subject transactions purportedly sourced from HKS. Rather, Cisco seeks virtually all of Dexon documents relating to PFT, irrespective of whether the subject products were sourced from HKS or involved the "particularly worrisome" switches Cisco relies on in support of its motions. Cisco admits it seeks such documents for the purpose of identifying and contacting Dexon's customers, and making extremely damaging and broad sweeping allegations of potential counterfeiting for all products. Cisco further admits it intends to demand some form of inspection and/or testing of all such products.

Recognizing the limited nature/scope of the HKS sourced products at issue, Cisco's motion also includes a vague, conclusory and confusing hearsay summary of purported deposition testimony from an unidentified "former employee" of an unidentified entity.

Dkt. 3, p. 5. No transcript of the actual testimony was furnished or provided. In addition to failing to identify the employee or his/her employer, the hearsay summary fails in any way to connect the alleged bad actions to PFT, any PFT products, or any of the documents sought by the subject subpoena. *Id.*

2. Duplicative and De Minimis Value

Cisco fails to explain, why, after well over a year's worth of discovery, including the full panoply of discovery available from the actual Defendants, it must now, at the last minute, track down and contact Dexon's end customers in order to prove its case. Any contention Cisco has not been afforded ample opportunity to date to procure and inspect alleged counterfeit product, and therefore now must be allowed to track down and contact Dexon's customers, lacks credibility.

In fact, any such argument is contradicted by Cisco's own admissions that it has already conducted significant third party discovery involving end user consumers known to be using the "particularly worrisome" switches. Without limitation, Cisco's submissions in the underlying litigation acknowledge it has already completed discovery involving multiple end users, including, without limitation, unidentified "government end users", the U.S. Army and West USA Realty. The Declaration of Richard Nelson provides:

> In 2019, Cisco subpoenaed various customers that purchased Cisco products from the Defendants. Many of the third parties cooperated with the subpoenas, and produced purchase orders, invoices, photographs, and electronic information from the products. Cisco engineers examined the photographs and electronic information and, in some situations, determined that the products sold by the Defendants were counterfeit.

Lafeber Dec., Ex. D, ¶5; *see also id.*, Ex. A., p. 2, n.1; Ex. B, p. 3.

Lastly, any attempt by Cisco to argue, as it did before the Northern District of California, that the scant few allegedly HKS sourced products sold by Dexon are somehow highly relevant and necessary to Cisco's damage calculations lacks merit. At the January 19, 2020 Case Management Conference, Cisco misleadingly labeled Dexon a "very substantial customer of the defendants" and claimed the subpoenaed documents were "obviously going to be really important for plaintiff's damage calculations." Lafeber Dec., Ex. D, Ex. 1, transcript pp. 11-12. Four (4) downstream sales of switches sourced from HKS by nonparty Dexon cannot reasonably be categorized as "really important for plaintiff's damage calculations."

III.
ARGUMENT

Federal Rule of Civil Procedure 45 provides that "[a] party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena." Fed. R. Civ. P. 45(c)(1). Rule 26 elaborates that "the court must limit the frequency or extent of discovery otherwise allowed. . .if it determines that:. . .the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive" or "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues." Fed. R. Civ. P. 26(b)(2)(C).

When discovery is sought from a non-party such as Dexon, the Court should be particularly sensitive to weighing the probative value of the information sought against the burden of production on the nonparty. *Datacard Sys., Inc. v. PacsGear, Inc.*, 2011 WL 2491366, at *2 (D. Minn. June 23, 2011); *see Misc. Docket Matter No. 1 v. Misc. Docket No. 2*, 197 F.3d 922, 927 (8th Cir. 1999) ("Concern for the burden upon non-parties carries 'special weight.'" (quoting *Cusumano v. Microsoft Corp.*, 162 F.3d 708, 717 (1st Cir. 1998)); *Fears v. Wilhelmina Model Agency, Inc.*, 2004 WL 719185, at *1 (S.D.N.Y. Apr. 1, 2004).

It is well-established that a court may "prohibit a party from obtaining discovery from a non-party if that discovery is available from another party to the litigation." *Gen. Parts Distribution, LLC v. Perry*, 2013 WL 3223374, at *4 (D. Minn. June 25, 2013) (citing *Arthrex, Inc. v. Parcus Med., LLC*, 2011 WL 6415540, at *6 (S.D. Ind. Dec. 21, 2011) ("A party's ability to obtain documents from a source with which it is litigating is a good reason to forbid it from burdening a non-party with production of those same documents.")); *see Phillip M. Adams & Assocs., L.L.C. v. Fujitsu Ltd.*, No. 1:05-cv-64 (TS), 2010 WL 1064429, at *3 (D. Utah Mar. 18, 2010) ("'Nonparty witnesses are powerless to control the scope of litigation and discovery, and should not be forced to subsidize an unreasonable share of the costs of a litigation to which they are not a party.'" (quoting *U.S. v. CBS, Inc.*, 666 F.2d 364, 371 (9th Cir. 1982)).

If a subpoena requires a non-party to search for and produce duplicative discovery that bears little on the claims for relief in the action, denying a response is proper. *See Everlight Elecs. Co. v. Nichia Corp.*, No. 13-mc-80251 (WHA), 2013 WL 6252530, at *5

(N.D. Cal. Dec. 3, 2013) ("[The Court] finds that these [nonparty] requests have little to no bearing on the claims for relief in the action" and that the requested discovery is "duplicative.")

Even if a request "is clearly relevant," it may nevertheless be denied because whether a request "is proportional is a separate inquiry." *See Nova Fin. & Inv. Corp. v. McDermott*, No. 18-cv-00075 (TUC/CKJ), 2018 WL 10399890, at *3 (D. Ariz. Oct. 29, 2018) ("Although it is possible for Bay to conduct a search query using those 5,000 Nova customers, the burden and expense likely outweighs the benefit of the proposed discovery – the mere possibility of discovering a communication implicating [Defendant] . . . . Since '[t]he purpose of the presently codified proportionality principle is to permit discovery of that which is needed to prove a claim or defense, but eliminate unnecessary or wasteful discovery', this request will not be permitted." (quoting *Crystal Lakes v. Bath & Body Works, LLC*, No. 2:16-cv-2989 (MCE/GGH), 2018 WL 533915, at *1 (E.D. Cal. Jan. 23, 2018)).

Subpoenas intruding upon a nonparty's confidentiality interests, including customer information, are routinely scrutinized and restricted. *See Tucker v. Am. Int'l Grp., Inc.*, 281 F.R.D. 85, 90 (D. Conn. 2012) (denying motion to compel non-party to produce documents, accepting non-party's argument that the subpoena "impermissibly and unnecessarily intrudes on the legitimate confidentiality interests of [the non-party] and its customers"). Moreover, "[t]he mere presence of a protective order does not by itself require disclosure of any kind"; rather, courts have routinely found that "a protective order is insufficient protection against unnecessary disclosure of confidential information to the

requesting party." *Lakeview Pharmacy of Racine, Inc. v. Catamaran Corp.*, No. 3:15-cv-290, 2017 WL 4310221, at *5; *see also Suture Express, Inc. v. Cardinal Health 200, LLC*, No. 14-cv-04737, 2014 WL 6478077, at *7 (N.D. Ill. Nov. 18, 2014) (restricting subpoena which would have resulted in damaging/harmful contact with customers).

In the present case, Cisco's motion should be denied on its face as untimely. In addition to Cisco's failure to act with the requisite diligence, the discovery sought is currently prohibited and not authorized under the applicable scheduling.

Cisco's motion is also substantively lacking. Specifically, Cisco's demand that nonparty Dexon search for, review, pull and produce any and all documents relating to PFT based solely on four (4) alleged sales sourced from HKS over a four (4) plus year period is both unreasonable and unjustified. Any arguable relevance and significance of such information is greatly outweighed by the harm to Dexon resulting from the disclosure of its confidential and trade secret information contained within the requested documents; namely its customers' identity.

It is *undisputed* Cisco intends to contact any disclosed Dexon customers and make unfounded and speculative allegations that the products purchased from Dexon – whether or not sourced from HKS – may be counterfeit. Worse, Cisco intends to harass Dexon customers further by demanding that such customers' currently "in use" products be subjected to some form of inspection and testing.

Even if Cisco had met its burden of establishing a likelihood that a significantly relevant portion of the subject Dexon products might be counterfeit, which it has not, it has utterly failed to demonstrate why the requested documents, and planned additional follow-

up discovery, is not duplicative to and necessary in light of prior third party discovery conducted by Cisco involving end consumers. The extremely limited number of Dexon sales allegedly sourced from HKS cannot realistically be considered necessary or instructive on either liability or damage issues.

IV.
CONCLUSION

Cisco's motion is both procedurally untimely and substantively lacking and should be denied in its entirety.

Dated: March 27, 2020

TAFT STETTINIUS & HOLLISTER LLP

By: */s/ Michael M. Lafeber*
Michael M. Lafeber (#242871
O. Joseph Balthazor Jr. (#0399093)
2200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
(612) 977-8400
mlafeber@taftlaw.com

ATTORNEYS FOR DEFENDANT DEXON COMPUTER, INC.